

What is claimed is:

1. A method, comprising:

obtaining information about a biometric part of a user's

body; and

forming a cryptographic key based on said biometric
information without determining absolute dimensions of said
biometric information.

2. A method as in claim 1 wherein said forming comprises
determining ratios between different portions of said biometric
information.

3. A method as in claim 1 further comprising entering a
plurality of different biometric features in a sequence, an order
of the sequence forming the code.

4. A method as in claim 1 further comprising entering
information that is supplemental to the biometric information,
the supplemental information indicating parts of the biometric
information which should be used to form the code.

1 5. A method as in claim 1, wherein said biometric part is
2 a fingerprint.

1 6. A method as in claim 4 wherein the supplemental
2 information includes an angle of a line used to obtain the
3 information.

1 7. A method comprising:
2 entering biometric information;
3 determining relationships between different parts of the
4 biometric information; and
5 using said relationships to form a cryptographic key.

1 8. A method as in claim 7 further comprising using said
2 cryptographic key to encrypt or decrypt information.

1 9. A method as in claim 8 wherein said relationship
2 includes a ratio between different parts of an image.

1 10. A method as in claim 8 wherein said biometric
2 information comprises a sequence of different items of biometric

3 information which are pieced together to form a code that is
4 dependent both on the pieces of the biometric information and on
5 the sequence.

a 1 11. An apparatus, comprising:

2 a biometric information obtaining part;

3 a computer;

4 wherein said computer is responsive to obtain an image from
5 the biometric information part, extract values from the biometric
6 information part, and use said values to encrypt or decrypt a
7 message.

1 12. An apparatus as in claim 11 wherein said computer
2 obtains a plurality of different biometric information parts, and
3 wherein both the content of the information parts and a sequence
4 of entry of the information parts, forms the code.

1 13. An apparatus as in claim 12 wherein the information is
2 formed by relationships between different parts of an image of
3 the biometric information.

1 14. A fingerprint sensor, comprising:

2 an image sensor chip forming a plurality of pixels for
3 sensing an image, said chip having an active surface which
4 receives said image, said active surface adapted to receive a
5 finger thereon to obtain a fingerprint therefrom and produce an
6 output indicative of the fingerprint.

1 15. A sensor as in claim 14 further comprising a computer
2 part, connected to said image sensor, receiving said output, and
3 using said output to form a cryptographic key.

1 16. A method as in claim 15 wherein said cryptographic key
2 is formed from a relationship between different parts of the
3 image.

1 17. A method, comprising:
2 obtaining information about a plurality of biometric parts
3 of a user's body;
4 forming a cryptographic key based on said information using
5 both the plurality of parts and a sequence of entry of the
6 plurality of parts; and
7 using said cryptographic key to one of encrypt or decrypt a
8 message.

1 18. A method as in claim 17 wherein said forming comprises
2 determining ratios between different portions of said biometric
3 information.

1 19. A method as in claim 17 further comprising entering
2 information that is supplemental to the biometric information,
3 the supplemental information indicating parts of the biometric
4 information which should be used to form the code.

1 20. A method as in claim 17, wherein said biometric part
2 is a fingerprint.

1 21. A method as in claim 19 wherein the supplemental
2 information includes an angle of a line used to obtain the
3 information.

1 22. A method, comprising:
2 obtaining information about a biometric part of a user's
3 body;
4 obtaining additional information; and
5 forming a cryptographic key based on both said biometric

6 information and said additional information.

a 1 23. A method as in claim 22 wherein said forming comprises
2 determining ratios between different portions of said biometric
3 information.

1 24. A method as in claim 22 further comprising entering a
2 plurality of different biometric features in a sequence, an order
3 of the sequence forming the code.

1 25. A method as in claim 22 wherein the supplemental
2 information includes an angle of a line used to obtain the
3 information.